IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

IN RE: HCA HEALTHCARE, INC. DATA SECURITY LITIGATION

Case No. 3:23 CV 684

MEMORANDUM OPINION

JUDGE JACK ZOUHARY

INTRODUCTION

Defendant HCA Healthcare experienced a cyberattack, later advising patients that hackers may have accessed personal and health information. Plaintiffs bring this putative class action. Plaintiffs jointly allege multiple theories of fault against Defendant, along with violations of various state consumer-protection statues (Doc. 120). Defendant moves to dismiss the Complaint under Federal Civil Rule 12(b)(6) (Docs. 127–28, 139). Plaintiffs oppose (Doc. 135).

BACKGROUND

Defendant is a large healthcare company comprised of 182 hospitals and over 2,300 care centers throughout the United States and the United Kingdom (Doc. 120 at ¶ 2). On July 5, 2023, Defendant discovered a cyberattack on its computer system (*id.* at ¶ 3). An unauthorized third party obtained Plaintiffs' and Class Members' personal identifiable information (PII) and protected health information (PHI) by hacking an external storage location -- used by Defendant for marketing email communications with patients (*id.* at ¶ 192). This data breach (Breach) included patient name, city, state, zip code, email, telephone number, date of birth, gender, patient service date, location of appointment, and date of next appointment (*id.* at ¶ 4). The hacker posted the stolen data dump consisting of 17 files and 27.7 million database records on a dark-web forum (*id.* at ¶¶ 193–94). The

hacker also included a ransom demand to Defendant, with a five-day deadline of July 10, 2023 (*id.*). After that date had passed, the hacker released the full database for sale (*id.*). While Defendant claims the information did not include any clinical, payment, or sensitive information, the dark web forum advertised that the data included "emails with health diagnosis that corresponds to a [C]lientID" (*id.* at ¶ 196).

On the deadline day, Defendant announced the cyberattack to the public through a posting on its website (*id.* at ¶ 195). Four days later, Defendant emailed some of the patients affected by the Breach (*id.*). In August 2023, Defendant sent out formal notices to affected patients to inform them of the Breach (*id.*). Defendant offered these patients free credit monitoring and identity-protection services for two years (*id.* at ¶ 197). Defendant claims that after discovering the attack, it "promptly disabled access to the external storage location [and] reported the crime to law enforcement" (Doc. 128 at 16).

ALLEGATIONS

Plaintiffs allege that the Breach resulted in increased spam calls and texts, unauthorized charges on their financial accounts, and fraudulent accounts opened in their names (Doc. 120 at ¶¶ 17–184). Plaintiffs also allege they have suffered lost time, annoyance, and money from monitoring and mitigating the impacts of the Breach (*id.* at ¶ 11). Their mitigation efforts include costs of identity-theft insurance, credit freezes/unfreezes, lost work time, fraud alerts, and decreased credit scores (*id.*).

Plaintiffs assert claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), breach of implied covenant of good faith and fair dealing (Count IV), breach of confidence (Count V), unjust enrichment (Count VI), and breach of fiduciary duty (Count VII). Plaintiffs also seek a declaratory judgment that Defendant failed to employ reasonable security

measures, and asks that Defendant implement industry-standard measures (Count VIII). Lastly, Plaintiffs assert statutory claims for the subclasses of individuals living in California, Florida, Kansas, Kentucky, Tennessee, and Virginia (Counts IX–XVI). (The Amended Complaint contains 16 counts. Count XV, brought under the Texas Deceptive Trade Practices - Consumer Protection Act, was voluntarily dismissed without prejudice (Doc. 129)).

LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), Defendant can move to dismiss a complaint for "failure to state a claim upon which relief can be granted." "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when [] plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* Determining plausibility is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.* at 679.

ANALYSIS

Defendant argues the Complaint contains three deficiencies that warrant dismissal across the board:

- Plaintiffs' alleged injuries are not legally cognizable.
- Plaintiffs fail to plausibly allege any wrongdoing.
- Defendant had no legal duty to control attacks perpetrated by criminal hackers.

Each of these arguments is addressed next.

SUFFICIENCY IN PLEADING - GENERAL

Cognizable Injury

Plaintiffs plead several purported injuries, but the primary one is identity theft. Defendant acknowledges Plaintiffs' express allegation, but argues that no particularly sensitive information, such as "account numbers, social security numbers, driver's license numbers, or passwords," was stolen such that it could plausibly cause the alleged injury (Doc. 128 at 22).

Although the severity of the Breach has yet to be determined, it is undisputed that -- at the very least -- PII such as names, birthdates, city, state, zip codes, and contact information were leaked (Doc. 128 at 46). "Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016). Plaintiffs do not need to be "literally certain" that their data will be misused, at least at this stage. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 415 n.5 (2013). The Sixth Circuit has not weighed in on the type of data necessary to find injury, but other circuits have found that even if a breach did not expose all the data necessary to inflict the alleged harms, leaked personal information "very well could have been enough to aid therein." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012).

At this stage, there is a sufficiently alleged substantial risk of harm -- mitigation costs resulting from the Breach. *Galaria*, 663 F. App'x at 388. This risk of harm due to the Breach, "coupled with reasonably incurred mitigation costs," is sufficient to establish cognizable injury. *Id.* For example, one Plaintiff alleges he has experienced identity theft since the Breach, citing incidents of fraudulent charges made on his financial and credit accounts (Doc. 120 at ¶ 22). Another Plaintiff alleges she was informed by her bank that her bank account attached to Defendant was subject to an attempted fraudulent purchase (*id.* at ¶ 69). Others recount credit cards opened in their names that they did not

personally open (*id.* at ¶ 89). These and other examples are sufficient to satisfy an increased risk of fraud and identity theft damages. *See In re Mednax Servs., Inc., Customer Data Sec. Breach Litig*, 603 F. Supp. 3d 1183, 1206 (S.D. Fla. 2022) (finding that "[e]ven a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement") (quoting *Resnick*, 693 F.3d at 1324).

As for the "reasonably incurred mitigation costs," Defendant claims Plaintiffs fail to plausibly allege actual financial loss, and that Defendant's self-initiated mitigation efforts foreclose any alleged financial damages. The Complaint alleges that Plaintiffs and Class Members have expended or otherwise expect to expend out-of-pocket expenses and lost opportunity costs associated with the prevention, detection, and consequences of the Breach (Doc. 120 at ¶ 11). Plaintiffs allege a continued risk and future costs in terms of time, effort, and money to mitigate and remedy the Breach (*id.*). The Sixth Circuit has recognized that the time and money expended to monitor credit, check bank statements, and modify financial accounts amount to sufficiently pled loss. *See Galaria*, 663 F. App'x at 389 (holding that "these costs [to monitor credit and obtain credit freezes] are a concrete injury suffered to mitigate an imminent harm" (citations and quotations omitted)).

Defendant's mitigation efforts do not erase Plaintiffs' individual efforts to remedy the Breach. Defendant's "$1,000,000 insurance reimbursement policy" does not cover the cost of credit monitoring and additional defense services (Doc. 120-1 at 3). Defendant counters that many courts do not treat allegations of lost time as a cognizable injury. But noted earlier, the Sixth Circuit suggests otherwise. *See Galaria*, 663 F. App'x at 388–89.

Alleged Wrongdoing

Defendant claims Plaintiffs fail to plead express facts supporting the claim that Defendant's "woefully inadequate security measures" gave rise to the Breach (Doc. 128 at 28). "The sufficiency

of a complaint turns on its 'factual content,' requiring the plaintiff to plead enough 'factual matter' to raise a 'plausible' inference of wrongdoing." *16630 Southfield Ltd. P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502, 504 (6th Cir. 2013) (quoting *Iqbal*, 556 U.S. at 678).

Plaintiffs expressly plead several facts that raise a plausible inference of wrongdoing, resulting in the Breach giving rise to this litigation. As to the adequacy of the security practices, Plaintiffs allege that Defendant failed to: "encrypt personal and sensitive data elements," "delete the Private Information it no longer had reason to maintain," and "audit its systems for vulnerabilities" (Doc. 120 at ¶¶ 9–12, 221–42, 256). Further, Plaintiffs' alleged harm of mitigating continued risk is supported by the express allegation that Defendant "has offered no assurances that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its security practices or dedicated sufficient resources and staff to avoid a similar breach of its network in the future" (*id.* at 3–4).

Defendant notes there are "obvious alternative explanations" for the attack (Doc. 128 at 30). But whether they are "obvious" or reasonable can only be determined by discovery. For now, it is certainly plausible Defendant failed to encrypt and timely delete sensitive data.

COMMON LAW CLAIMS

Plaintiffs' tort and contract claims are based in state law. *See Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 495–98 (1941). The parties make mention of the applicable state law because the Breach affected Plaintiffs residing in various states, including California, Florida, Kansas, Kentucky, Tennessee, Texas, and Virginia (Doc. 120 at ¶¶ 17–184). This Court will need to engage in a choice-of-law analysis, but not at this stage of the case. *See Wise v. Zwicker & Assocs., P.C.*, 780 F.3d 710, 718 (6th Cir. 2015) (reversing dismissal of a claim where "[t]he pleadings do not provide sufficient facts to make a determination on the . . . [choice-of-law] issues"). This Court does

not have sufficient information at this early juncture to engage in a comprehensive choice-of-law analysis. Because no conflict exists "between the relevant laws of the different jurisdictions," this Court looks to the parties' cited authority for the purposes of this Motion. *Boswell v. RFD-TV the Theater, LLC*, 498 S.W.3d 550, 555 (Tenn. Ct. App. 2016).

Tort Claims

Defendant broadly challenges all tort claims, relying on Florida law in arguing it had "no duty to prevent the misconduct of third persons," particularly when the conduct was a crime. *Jackson Hewitt, Inc. v. Kaman*, 100 So.3d 19, 28 (Fla. Dist. Ct. App. 2011) (citation omitted). However, Florida precedent holds that negligence liability may be imposed on the basis of affirmative acts which allow an "unreasonable risk of harm by creating a foreseeable opportunity for third party criminal conduct," even without any "special relationship" between the parties that independently imposes a duty to warn or guard against that misconduct. *United States v. Stevens*, 994 So. 2d 1062, 1068 (Fla. 2008). This is nearly identical to Plaintiffs' relied-upon Tennessee precedent, which holds that "all persons have a duty to use reasonable care to refrain from conduct that will foreseeably cause injury to others." *Bradshaw v. Daniel*, 854 S.W.2d 865, 870 (Tenn. 1993). "One who assumes to act, even though gratuitously, may thereby become subject to the duty of acting carefully." *Biscan v. Brown*, 160 S.W.3d 462, 482–83 (Tenn. 2005). Plaintiffs plead the Breach was foreseeable, and that Defendant affirmatively created, collected, and stored Plaintiffs' PII/PHI (Doc. 120 at ¶¶ 213, 219, 250, 369). This is sufficient to establish duty for Plaintiffs' negligence claims.

Defendant then individually challenges Plaintiffs' tort claims, each addressed next.

Negligence (Count I). Defendant argues Plaintiffs' negligence claims fail because Plaintiffs fail to allege cognizable injury causally attributable to Defendant, and because Defendant had no duty

to prevent criminal acts by third parties. For reasons discussed above, Plaintiffs sufficiently plead duty and injury-in-fact; these arguments fail.

Defendant also argues that Tennessee law imposes no duty to guard against purely economic losses. As Plaintiffs point out, this argument is misleading. Tennessee courts have found "no compelling reason to extend the economic loss doctrine to services contracts." *Com. Painting Co. Inc. v. Weitz Co. LLC*, 676 S.W.3d 527, 538 (Tenn. 2023). Plaintiffs' negligence claim stands.

Negligence Per Se (Count II). Plaintiffs allege Defendant had duties arising under the Health Insurance Portability and Accountability Act (HIPAA), the HIPAA Privacy and Security Rule, and Section 5 of the Federal Trade Commission (FTC) Act. The parties rely on Tennessee law to define the requirements of a negligence-per-se claim. Among other factors, this Court must consider "whether the statute clearly defines the prohibited or required conduct." *Rains v. Bend of the River*, 124 S.W.3d 580, 591 (Tenn. Ct. App. 2003). *See also* Restatement (Second) of Torts § 874A cmt. h(1). They do not.

The Sixth Circuit has held that HIPAA does not establish an independent duty under Tennessee law or otherwise establish a private means of enforcement. *See Faber v. Ciox Health, LLC*, 331 F. Supp. 3d 767, 779–80 (W.D. Tenn. 2018), *aff'd*, 944 F.3d 593 (6th Cir. 2019). Because HIPAA is not applicable here, this Court need not decide whether Defendant violated any of its provisions.

Section 5 of the FTC Act broadly prohibits "unfair methods of competition in or affecting commerce." 15 U.S.C. § 45(a)(1). Plaintiffs allege Defendant engaged in acts or omissions declared "unfair trade practices" by the FTC. In support, they claim the "FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by

Plaintiffs and the Class" (Doc. 120 at ¶ 287). This argument is self-defeating. "By relying on extra-statutory sources to determine what constitutes an 'unfair' cybersecurity practice, [Plaintiffs] implicitly concede[] that the statute itself provides no such answer." *Allen v. Wenco Mgmt., LLC*, 696 F. Supp. 3d 432, 440 (N.D. Ohio 2023). Count II is dismissed.

Breach of Confidence (Count V). Plaintiffs allege "Tennessee has long recognized a cause of action for breach of confidential relationship" (Doc. 135 at 37). Plaintiffs also acknowledge that, under Tennessee law, a confidential relationship is found where the stronger party exercised "dominion and control" over the weaker party. *Heflin v. Iberiabank Corp.*, 571 S.W.3d 727, 736 (Tenn. Ct. App. 2018). Plaintiffs do not plead, generally or by express facts, that Defendant had dominion and control over Plaintiffs. The elements of a claim for breach of confidential relationship are: "(1) the defendant was in a position to influence or control the plaintiff; (2) the defendant used the confidences given . . . to obtain some benefit from, or advantage over, the plaintiff; and (3) the plaintiff . . . suffered some detriment at the hands of the defendant." *Id.* (citation omitted). Because the Complaint does not contain the elements for breach of confidential relationship, Count V is dismissed as well.

Breach of Fiduciary Duty (Count VII). Plaintiffs' final tortious claim alleges Defendant breached its fiduciary duties by failing to properly protect Plaintiffs' PII and further by failing to detect the Breach and notify Plaintiffs (Doc. 120 at ¶ 350). Plaintiff alleges Defendant became a fiduciary "by its undertaking and guardianship of Plaintiffs' and Class Members' [PII] to act primarily for their benefit" (*id.* at ¶ 347). Tennessee law recognizes two types of fiduciary relationship: "fiduciary per se, 'such as between a guardian and ward, an attorney and client, or conservator and incompetent,'" and other relationships in which "one party exercise[s] 'dominion and control over another.'" *Grant v. Tucker*, 57 F. Supp. 3d 852, 859 (M.D. Tenn. 2014) (citation omitted).

Plaintiffs appear to allege a "guardian-ward" relationship. Courts have rejected this argument in the context of data breaches. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1146 (C.D. Cal. 2021) (finding the defendant genetic-testing company "never agreed to subordinate [their] interests to those of Plaintiffs, and Plaintiffs were not so vulnerable as to give rise to equitable concerns underlying the protection afforded by law governing fiduciaries") (cleaned up)). Accordingly, Count VII is dismissed.

Breach-of-Contract Claims

Plaintiffs allege they entered into implied contracts with Defendant by entrusting their PII with the understanding that Defendant would reasonably safeguard that information from unauthorized access or disclosure (Doc. 120 at ¶ 296). Defendant argues the contract claims are barred because Plaintiffs fail to point to any explicit promise made by Defendant to "safeguard and protect Plaintiffs' information from criminal hackers" (Doc. 128 at 34). Defendant improperly focuses on the criminal nature of the Breach, rather than its own actions that may have given rise to the Breach. At issue is whether Defendant impliedly agreed to protect the PII/PHI from any unauthorized access -- criminal or otherwise. Without discovery it is unknown whether the hackers employed tactics beyond what Defendant could have reasonably anticipated in its security measures. Accordingly, the claims are not automatically barred and this Court must next evaluate the sufficiency of the pleading.

Breach of implied contract (Count III). "A contract implied in fact is one that 'arises under circumstances which show mutual intent of assent to contract.'" *Thompson*, 136 S.W.3d at 930 (citation omitted). "[F]or a contract implied-in-fact to be enforceable, it must be supported by mutual assent, consideration, and lawful purpose." *Id*. "It is well-settled that consideration exists when the promisee does something that it is under no legal obligation to do or refrains from doing something

which it has a legal right to do." *GuestHouse Int'l, LLC v. Shoney's N. Am. Corp.*, 330 S.W.3d 166, 188 (Tenn. Ct. App. 2010).

Plaintiffs' efforts to create and impose an implied-in-fact contract rest on Defendant's legal obligations under federal and state statutes. But the Complaint fails to show any agreement outside of the pre-existing obligations imposed by statute. Plaintiffs point to the Notices of Privacy Practices that govern Defendant-owned hospitals, which states Defendant is "required by law to maintain the privacy of [Plaintiffs'] health information" (Doc. 120 at ¶ 294). This is not like *Clemens v. ExecuPharm Inc.*, where the employment agreement expressly contracted "to take appropriate measures to protect . . . confidentiality and security." 48 F.4th 146, 156 (3d Cir. 2022). There is no such provision here. As Defendant states, Plaintiffs "transacted to receive healthcare services from Defendant -- not data security services beyond the privacy requirements already imposed on Defendant by federal law." *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1369 (SD. Fla. 2017). This claim is therefore dismissed.

Breach of implied covenant of good faith and fair dealing (Count IV). Plaintiffs concede that under Tennessee law, breach of the implied covenant of good faith and fair dealing is not a standalone cause of action and is subsumed by their claim for breach of implied contract (Doc. 135 at 40). *See Davidson v. Arlington Cmty. Sch. Bd. of Educ.*, 847 F. App'x 304, 310 (6th Cir. 2021) (holding that "in Tennessee, breach of the implied covenant of good faith and fair dealing is not an independent basis for relief") (cleaned up). Because the underlying claim for breach of implied contract is dismissed, so too is this claim.

Unjust enrichment (Count VI). Alternatively, Plaintiffs plead unjust enrichment (Doc. 120 at ¶ 336). Plaintiffs allege that Defendant has been unjustly enriched through the retention of

Plaintiffs' private information (*id.* at ¶ 339). As for their factual assertions, they only allege that "HCA profited from Plaintiffs' retained data" and used it "for business purposes" (*id.* at ¶ 338).

Tennessee courts have found that this cause of action must be based on circumstances "much more specific" than simply stating Defendants were enriched in an unjust manner. *Wachter, Inc. v. Cabling Innovations, LLC*, 387 F. Supp. 3d 830, 847 (M.D. Tenn. 2019). Plaintiffs do not sufficiently allege facts that plausibly explain how Defendants were enriched by possession of Plaintiffs' PII. The unjust enrichment claim fails as a matter of law, and Count IV is dismissed.

STATUTORY CLAIMS

Finally, Defendants argue Plaintiffs' seven statutory claims must be barred for reasons already discussed -- namely, the criminal nature of the Breach. For the reasons stated above, the statutory claims are not automatically foreclosed. Each is evaluated in turn below:

California Conf. of Med. Information Act (Count IX). Defendants argue Plaintiffs' claim under the CMIA is deficient because Plaintiffs do not allege any factual affirmative conduct. Cal. Civ. Code § 56.05(i). The CMIA requires Defendant to have disclosed "medical information" which in turn demands "an affirmative act of communication" by Defendant." *Regents of Univ. of Cal. v. Super. Ct.*, 220 Cal. App. 4th 549, 564 (2013). Plaintiffs allege that Defendant affirmatively acted by "disclos[ing] medical information" (Doc. 120 at ¶ 368). Defendant's opposition rests on its insistence that it did not communicate the information. But the details the Breach are not yet known. Plaintiffs' claim is well-pleaded and therefore survives.

California Unfair Competition Law "UCL" (Count X). Despite Defendant's argument that Plaintiffs failed to plead sufficient facts explaining how Defendant may have acted unlawfully, unfairly, or deceptively, Plaintiffs expressly cite to Defendant's failure to implement reasonable security measures and to identify foreseeable risks (Doc. 120 at ¶¶ 403–04).

Defendant also argues Plaintiffs fail to plead "economic loss." Named Plaintiff in this claim alleges he subscribed to a monthly credit monitoring service, at a cost. Defendant acknowledges Plaintiffs' pleading, but argues the incurred costs were unnecessary in light of Defendant's offered credit-monitoring services. However, "[t]o the extent that [Defendant] factually disputes whether [Plaintiffs'] credit monitoring costs were 'required' or 'necessary,' that cannot be resolved at this [motion to dismiss] stage." *Schmitt v. SN Servicing Corp.*, 2021 WL 3493754, at *8 (N.D. Cal. 2021). It may be that Plaintiffs have only nominal damages. Time will tell.

Florida Deceptive and Unfair Trade Practices Act "FDUTPA" (Count XI). Defendant's arguments regarding Plaintiffs' claims brought under the FDUTPA mirror those regarding the UCL claims. Plaintiffs sufficiently point to factual allegations that Defendant failed to implement and maintain reasonable security measures, and failed to identify and remediate foreseeable security and privacy risks. Plaintiffs also allege throughout the Complaint that Defendant experienced prior cybersecurity incidents and should have responded accordingly to avoid the Breach at hand.

Defendant also argues the FDUTPA permits recovery only for "actual damages." Not so. As recognized in *Tymar Distrib. LLC v. Mitchell Grp. USA, LLC*, there is "a much larger universe of damages available in FDUTPA claims arising outside the consumer transaction context . . . especially when considered alongside the liberal construction courts must afford the FDUTPA to accomplish its remedial purpose." 2021 WL 4077966, at *7 (S.D. Fla. 2021). In *Tymar*, the court held actual or compensatory damages are those which "arise from actual and indirect pecuniary loss, mental suffering, value of time, actual expenses, and bodily pain and suffering." Plaintiffs sufficiently plead pecuniary loss, mental suffering, value of time, and actual expenses.

Kansas Consumer Protection Act "KCPA" (Count XII). The KCPA prohibits deceptive and unconscionable acts or practices in connection with a consumer transaction. K.S.A. §§ 50–626(a);

627(a). Defendant argues Plaintiffs fail to plead with particularity "deceptive" or "unconscionable" conduct. However, "KCPA claims need not be pleaded with particularity." *Tomlinson v. Ocwen Loan Servicing, LLC*, 2015 WL 7853957, at *2 (D. Kan. 2015).

Rather, Kansas law "requires courts to liberally construe the statute to promote the policy of protecting consumers from suppliers who commit deceptive and unconscionable practices." *Nieberding v. Barrette Outdoor Living, Inc.*, 2012 WL 6024972, at *5 (D. Kan. 2012) (citing Kan. Stat. Ann. § 50–623(b)). "Typically, unconscionable acts or practices involve conduct seek[ing] to . . . require a consumer to assume risks which materially exceed the benefits of a related consumer transaction." K.S.A. § 50–627, 1973 cmt. 1. Plaintiffs allege they were required to assume the risk of Defendant's deceptive and unconscionable conduct by providing their personal information in exchange for health services. Plaintiffs sufficiently allege Defendant failed to comply with common law and statutory duties, as well as misrepresented it would protect privacy and confidentiality.

Kentucky Consumer Protection Act "CPA" (Count XIII). The Kentucky CPA prohibits "[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce." Ky. Rev. Stat. § 367.170(1). Defendant claims the Kentucky Plaintiff fails to plausibly allege "any substantial wrong" that would support liability (Doc. 128 at 49).

Named Plaintiff pleads that Defendant knew the risk of cybersecurity incidents but still failed to implement and maintain the necessary protection measures. Plaintiff also pleads that even after the Breach occurred and the risk was apparent, Defendant failed to improve the security and privacy measures that gave rise to this Breach. Contrary to Defendant's assertions, these factual allegations are not generic. The specifics of Defendant's actions, and whether these actions are unfair, false, or misleading is a question better answered after discovery. *See M.T. v. Saum*, 7 F. Supp. 3d 701, 705

(W.D. Ky. 2014). As acknowledged by Defendant, the same is true for Plaintiffs' allegation of a $300 pecuniary loss.

Defendant also argues Plaintiff cannot maintain a class action under the Kentucky CPA. But "[t]here is no explicit prohibition of class actions . . . anywhere . . . in the [Kentucky CPA]." *Kempf v. Lumber Liquidators, Inc.*, 2017 WL 4288903, at *3 (W.D. Ky. 2017). "[C]lass actions under the [Kentucky CPA] have been previously certified by [district courts] and Kentucky state courts on several occasions," and the venue provisions of the CPA "do not prohibit class actions." *Id.* at *3–4.

Tennessee Consumer Protection Act (Count XIV). Defendant repeats its argument that Tennessee Plaintiff pleads no facts supporting an unfair or deceptive claim under the Tennessee CPA. "To state a claim under the Tennessee Consumer Protection Act ("TCPA"), [a] plaintiff must allege that the defendant engaged in an unfair or deceptive act or practice." *Asurion, LLC v. SquareTrade, Inc.*, 407 F. Supp. 3d 744, 751 (M.D. Tenn. 2019).

Plaintiff sufficiently plead Defendant knew about the heightened security risks as a result of prior data breaches but still failed to implement and maintain reasonable security and privacy measures. Again, discovery may answer whether this conduct is "unfair," "deceptive," or even accurate. *Id.* (quoting *Cloud Nine, LLC v. Whaley*, 650 F. Supp. 2d 789, 798 (E.D. Tenn. 2009)). For now, the pleading is sufficient to survive dismissal.

Virginia Consumer Protection Act (Count XVI). Defendant raises the same arguments of pleading with particularity, actual damages, and reimbursements. For the reasons set forth above, Plaintiff sufficiently pleads the requirements for a VCPA claim.

DECLARATORY JUDGMENT

Finally, Defendant argues Plaintiffs' claim brought under the Declaratory Judgment Act (DJA) must be dismissed because it cannot be brought as a standalone action. Defendant also argues

Plaintiffs' request for declaratory judgment belongs in their prayer for relief, and should not be a separate count (Doc. 128 at 55). To satisfy the pleading requirements of the DJA, Plaintiffs must "plausibly alleg[e] facts that, 'under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.'" *Saginaw Cnty., Michigan v. STAT Emergency Med. Servs., Inc.*, 946 F.3d 951, 954 (6th Cir. 2020) (quoting *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007)). However, the purpose of the DJA is to "create an alternative remedy," and that is not necessary here as Plaintiffs have viable damages claims. *Id.*

Plaintiffs allege Defendant is still in possession of their PII/PHI but has yet to implement adequate security measures. 28 U.S.C. §§ 2201, *et seq.* Plaintiffs request this Court enter a judgment declaring Defendant owes a legal duty to secure the PII/PHI and that Defendant has been in continued breach of this legal duty. Plaintiffs then request 13 equitable remedies, each detailing some affirmative conduct it requests from Defendant. All of these requests may be brought in the form of a request for injunctive relief. The DJA is not an appropriate cause of action for the claims remaining in this case.

CONCLUSION

The Complaint provides sufficient factual information to support a claim of negligence. The Motion to Dismiss (Doc. 128) is denied as to that claim (Count I) and corresponding violations of state statutes (Counts IX–XVI). The remaining counts (II–VIII) are dismissed.

IT IS SO ORDERED.

s/ *Jack Zouhary*
JACK ZOUHARY
U. S. DISTRICT JUDGE

August 15, 2024